

IRREDUCIBILITY AND EMBEDDING PROBLEMS

LIOR BARY-SOROKER

ABSTRACT. We study irreducible specializations, in particular when group-preserving specializations may not exist. We obtain a criterion in terms of embedding problems. We include several applications to analogs of Schinzel's hypothesis H and to the theory of Hilbertian fields.

1. INTRODUCTION AND RESULTS

A Hilbertian field K is defined by the property that every finite family of polynomials

$$f_1(T_1, \dots, T_r, X), \dots, f_s(T_1, \dots, T_r, X)$$

in the ring $K[T_1, \dots, T_r, X]$ (where $r \geq 1$ is arbitrary) that are irreducible and separable in X admits an irreducible specialization: $(a_1, \dots, a_r) \in K^r$ such that all $f_i(a_1, \dots, a_r, X)$ are irreducible in $K[X]$. The set of irreducible specializations is Zariski dense in K^r . Hilbert's irreducibility theorem asserts that a number field is Hilbertian, and Kuyk's theorem asserts that Hilbertianity is preserved under abelian extensions, for a more general permanence criterion, the so called Haran's diamond theorem, see [9].

We write in short \mathbf{T} for (T_1, \dots, T_r) , and similarly for other tuples. If K is Hilbertian, then a strictly stronger specialization property holds, namely there exist group-preserving specializations: $\mathbf{a} \in K^r$ such that

$$\text{Gal}(f(\mathbf{T}, X), K(\mathbf{T})) \cong \text{Gal}(f(\mathbf{a}, X), K)$$

as permutation groups, where $f(\mathbf{T}, X) = \prod_{i=1}^s f_i(\mathbf{T}, X)$. This implies that in order to realize a finite group over a Hilbertian field K it suffices to realize the group over $K(\mathbf{T})$, which is easier since we have more degrees of freedom and geometry comes into the play, cf. [15, 11, 16].

Nevertheless, in many applications the irreducible specialization property suffices. For example, in [14, 17] Scharlau and Waterhouse (independently) prove that over a Hilbertian field every non-degenerate quadratic form is isomorphic to a scaled trace form. In the proof the irreducible specialization property is applied to the characteristic polynomial $f(\mathbf{T}, X)$ of \mathcal{TB} , where $\mathcal{T} = (T_{i,j})$ is the generic symmetric matrix of order n (i.e., the entries $T_{i,j}$ are variables subject to the relations $T_{i,j} = T_{j,i}$) and B is a non-degenerate symmetric matrix of order n with coefficients lying in K .

In [5] Kelmer and the author show that $\text{Gal}(f(\mathbf{T}, X), \tilde{K}(\mathbf{T})) \cong S_n$, where \tilde{K} denotes an algebraic closure of K . Thus the result holds true over a much wider family of fields, see below. In this case one can think of f as “the most irreducible-in- X ” polynomial. This is what one expects to come out of generic constructions.

Another application appears in [2] where the author addresses an analog of Dirichlet's theorem on primes in arithmetic progressions for polynomial rings. Let $a(X), b(X) \in K[X]$ be relatively prime polynomials, then for any $m \gg \deg(a), \deg(b)$, there exists $c(X)$ of degree m (let $n = m - \deg(b) = \deg_X(a(X) + Tb(X)c(X))$) such that

$$\text{Gal}(a(X) + Tb(X)c(X), \tilde{K}(T)) \cong S_n.$$

So an irreducible specialization induces an irreducible in the ‘arithmetic progression’ $a(X) + b(X)K[X]$.

In both of these applications the property the field K needs to satisfy is the irreducible specialization property for “the most irreducible-in- X ” polynomials. [2] gives a sufficient condition

to have irreducible specializations in this case in terms of pseudo algebraically closed (PAC) extensions.

Theorem 1.1. *Let K be a field and let $f(\mathbf{T}, X) \in K[\mathbf{T}, X]$ be a separable polynomial of degree n in X such that*

$$\text{Gal}(f(\mathbf{T}, X), \tilde{K}(\mathbf{T})) \cong S_n.$$

Assume K has a PAC extension having a separable extension of degree n . Then there exists a Zariski dense set of $\mathbf{a} \in K^r$ such that $f(\mathbf{a}, X)$ is irreducible in $K[X]$.

A PAC extension M/K is defined by the property that for every absolutely irreducible M -variety V of dimension $r \geq 1$ and for every dominating separable M -map $\nu: V \rightarrow \mathbb{A}^r$ there exists $\mathbf{a} \in V(M)$ such that $\nu(\mathbf{a}) \in K^r$.

In [5] Kelmer and the author prove that some interesting families of algebraic extensions of a countable Hilbertian field have PAC extensions. For example, let K be a pro-solvable extension of a countable Hilbertian field. Then there exists a PAC extension M/K having a separable extension of arbitrary degree $n \geq 5$. In particular we can take $K = \mathbb{Q}_{\text{sol}}$. This field is not Hilbertian because it has no quadratic extensions, so $X^2 - T$ has no irreducible specialization. Also S_n does not occur as Galois group over \mathbb{Q}_{sol} . So there is no group-preserving specialization for a polynomial as in Theorem 1.1, although there are irreducible specializations.

In this work we study more deeply irreducible specializations, in particular when group-preserving specializations do not exist.

Let $f_1(\mathbf{T}, X), \dots, f_s(\mathbf{T}, X) \in K[\mathbf{T}, X]$ be distinct irreducible polynomials that are separable in X and let $f = f_1 \cdots f_s$. Then f is separable in X . Now f defines the **associated geometric embedding problem** for K that we denote by $\mathcal{E}(f, K)$: Let F be the splitting field of $f(\mathbf{T}, X)$ over $K(\mathbf{T})$ and let $L = F \cap \tilde{K}$. Then both $F/K(\mathbf{T})$ and L/K are Galois extensions. Let $H = \text{Gal}(F/K(\mathbf{T}))$, $G = \text{Gal}(L/K)$, and let $\alpha: H \rightarrow G$ and $\rho: \text{Gal}(K) \rightarrow G$ be the restriction maps. The diagram

$$\begin{array}{ccc} & & \text{Gal}(K) \\ & & \downarrow \rho \\ H & \xrightarrow{\alpha} & G \end{array}$$

defines the embedding problem $\mathcal{E}(f, K)$.

If $\text{Gal}(f, \tilde{K}(\mathbf{T})) = S_n$, for some polynomial $f(\mathbf{T}, X)$ of degree n in X , then the associated geometric embedding problem is

$$\begin{array}{ccc} & & \text{Gal}(K) \\ & & \downarrow \rho \\ S_n & \xrightarrow{\alpha} & 1. \end{array}$$

Theorem 1.2. *Let K be a field, $f_1(\mathbf{T}, X), \dots, f_s(\mathbf{T}, X) \in K[\mathbf{T}, X]$ distinct irreducible polynomials that are separable in X , $f = f_1 \cdots f_s$, and for each i let x_i be a root of $f_i(\mathbf{T}, X)$ in a fixed algebraic closure of $K(\mathbf{T})$. Assume there exist a PAC extension M/K and a solution $\eta: \text{Gal}(M) \rightarrow \text{Gal}(f(\mathbf{T}, X), M(\mathbf{T}))$ of $\mathcal{E}(f, M) = (\rho, \alpha)$ with image $H_0 = \eta(\text{Gal}(M))$ such that*

$$(H_0 \cap C)x_i = Cx_i,$$

for some $\ker \alpha \leq C \leq \text{Gal}(f(\mathbf{T}, X), M(\mathbf{T}))$. Then there exists a Zariski dense set of $\mathbf{a} \in K^r$ such that all $f_i(\mathbf{a}, X)$ are irreducible.

Remark 1.3. Here are two properties of η which imply the existence of C as in Theorem 1.2.

If η is **surjective**, i.e. $H_0 = \text{Gal}(f(\mathbf{T}, X), M(\mathbf{T}))$, then trivially we have $(H_0 \cap C)x_i = Cx_i$.

Assume H_0 acts **transitively** on the set R_i of the roots of $f_i(\mathbf{T}, X)$. Let $C = \text{Gal}(f(\mathbf{T}, X), M(\mathbf{T}))$. We have $(H_0 \cap C)x_i = H_0x_i = R_i$. On the other hand, $H_0x_i \subseteq Cx_i \subseteq R_i$. So $(H_0 \cap C)x_i = Cx_i (= R_i)$.

Remark 1.4. Theorem 1.2 generalizes Theorem 1.1 since under Theorem 1.1 assumptions, $\mathcal{E}(f, M) = (\text{Gal}(M) \rightarrow 1, S_n \rightarrow 1)$. This embedding problem has a solution the image of whose is transitive if and only if M has a separable extension of degree n .

Remark 1.5. In the special case when K is a PAC field (i.e. $K = M$) and $C = \text{Gal}(f(\mathbf{T}, X), M(\mathbf{T}))$, Theorem 1.2 becomes sharp, see [4].

The proof of Theorem 1.2 is based on the *lifting property* of PAC extensions [3]. This property allows us to lift a solution of $\mathcal{E}(f, M)$ to a solution of $\mathcal{E}(f, K)$ that is *geometric*, i.e., is induced by a specialization $\mathbf{T} \mapsto \mathbf{a} \in K^r$. See Section 2.3

Theorem 1.2 is very applicable. To demonstrate this we include three applications.

Schinzel's Hypothesis H predicts that a family of polynomials with integral coefficients admits infinitely many simultaneous prime values in \mathbb{Z} under some necessary conditions. Analogs for polynomial rings was considered in [7, 6, 12, 4].

In [6] Bender and Wittenberg obtain a geometric sufficient condition for a family of irreducible polynomials with two variables T, X with coefficients in a large finite field to admit simultaneous irreducible values in $\mathbb{F}_q[T]$. The following result extends [6] to the family of fields having PAC extensions.

Theorem 1.6. *Let K be a field of characteristic $p \geq 0$, let $f_1(T, X), \dots, f_s(T, X) \in K[T, X]$ be irreducible polynomials. Assume that the Zariski closure $C_i \subseteq \mathbb{P}^2$ of the affine curve $\{f_i = 0\} \subseteq \mathbb{A}^2$ is smooth for every $i = 1, \dots, s$ and that $p \nmid d_i(d_i - 1)$, where d_i is the total degree of f_i . Assume there exists a PAC extension M/K having a separable extension of degree d_i , for every $i = 1, \dots, s$. Then there exist infinitely many $(a, b) \in K^2$ such that all $f_i(T, aT + b)$ are irreducible in $K[T]$.*

Here apart of Theorem 1.2 we use a calculation of a Galois group due to Bender and Wittenberg.

It is interesting to note that Theorem 1.6 implies [6]. This is done by applying Theorem 1.6 in the case K is pseudo finite, $K = M$, and then applying Ax's theorem on the elementary theory of finite fields [1], see Section 4.2.

The second application generalizes a result of Pollack [12] and the author [4].

Theorem 1.7. *Let K be a field of characteristic $p \geq 0$, let $n > 0$ be an integer such that n is odd if $p = 2$, and let $f_1(X), \dots, f_s(X) \in K[X]$ be non-associate irreducible separable polynomials with respective roots $\omega_1, \dots, \omega_s$. Assume there exists a PAC extension M/K such that $M(\omega_i)$ has a degree n separable extension, for every $i = 1, \dots, s$. Then there exists a Zariski dense set of $(a_1, \dots, a_n) \in K^n$ such that for $g(T) = T^n + a_1 T^{n-1} + \dots + a_n$ all $f_i(g(T))$ are irreducible.*

Here we need a calculation of Galois groups that appears in [4] in order to apply Theorem 1.2.

Remark 1.8. In [4] the author proves Theorem 1.7 for PAC fields (i.e., $K = M$). In the case when K is also pseudo finite, i.e. PAC, $\text{Gal}(K) = \widehat{\mathbb{Z}}$, and K is perfect, a more precise result is obtained. Then using Ax' theorem it follows that if $K = \mathbb{F}_q$ is a finite field of characteristic p , and if n is an integer, odd if $p = 2$, then

$$\#\{(a_1, \dots, a_n) \in \mathbb{F}_q^n \mid \text{all } f_i(t^n + a_1 t^{n-1} + \dots + a_n) \text{ are irreducible}\} = q^n + O(q^{n-\frac{1}{2}}).$$

Here the asserted constant depends on the sum of the degrees of f_1, \dots, f_s and on n .

This extends the previous result [12], in which Pollack establishes the asymptotic formula under the assumptions $p \neq 2$ and $p \nmid n$.

These two applications make the property that a field K has a PAC extension M/K with 'many' separable extensions interesting. As mentioned above, in [5], this property was studied, and some examples were given. E.g., pro-solvable extensions of a countable Hilbertian field ($n \geq 5$) and more. We hope that this work will motivate further study of PAC extensions.

The last result applies the theory of PAC extensions to the theory of Hilbertian fields. It is known that if K is a countable Hilbertian field, then for every $n \geq 1$ there is an abundance of PAC extensions M/K such that $\text{Gal}(M)$ is a free profinite group of rank n [10]. We prove a strong converse.

Theorem 1.9. *Let K be a field. Assume that for infinitely many $n \geq 1$ there exists a PAC extension M/K with $\text{Gal}(M)$ free of rank $\geq n$. Then K is Hilbertian.*

Remark 1.10. Razon proves that if K has a PAC extension M with $\text{Gal}(M)$ free of infinite rank, then M is Hilbertian over K , and in particular K is Hilbertian [13, Corollary 2.6].

2. BACKGROUND

We briefly recall the definition of geometric embedding problems and of double embedding problems and we formulate the lifting property of PAC extensions. This property plays a crucial role in the proof of Theorem 1.2. Full details appear in [3], cf. [4].

2.1. Geometric embedding problems. Let K be a field, K_s a separable closure of K , and $\text{Gal}(K) = \text{Gal}(K_s/K)$ the absolute Galois group of K . A finite embedding problem \mathcal{E} for K consists on an epimorphism of finite groups $\alpha: H \rightarrow G$ and an epimorphism¹ $\rho: \text{Gal}(K) \rightarrow G$. In short we write $\mathcal{E} = (\rho, \alpha)$. A weak solution is a homomorphism $\theta: \text{Gal}(K) \rightarrow H$ such that $\alpha\theta = \rho$. If θ is surjective, we say that θ is a proper solution.

$$\begin{array}{ccc} & & \text{Gal}(K) \\ & \swarrow \theta & \downarrow \rho \\ G & \xrightarrow{\alpha} & G \end{array}$$

Assume that E is a finitely generated regular extension of K , and let F/E be a finite Galois extension. Then $L = F \cap K_s$ is Galois over K and

$$\mathcal{E}(F/E, K) = (\rho: \text{Gal}(K) \rightarrow \text{Gal}(L/K), \alpha: \text{Gal}(F/E) \rightarrow \text{Gal}(L/K)),$$

with ρ, α the restriction maps, is a finite embedding problem for K (note that E/K regular implies that α is surjective). These embedding problems are called **geometric**. If $E = K(\mathbf{T})$, for some tuple $\mathbf{T} = (T_1, \dots, T_r)$ of algebraically independent variables, we call the embedding problem $\mathcal{E}(F/K(\mathbf{T}), K)$ **rational**.

Let φ be a K -place of E (i.e. $\varphi(x) = x$, for all $x \in K$). Assume that the residue field of φ is K and that φ is unramified in F . Then every L -place Φ of F that prolongs φ defines a solution Φ^* of $\mathcal{E}(F/E, K)$ by the formula

$$(1) \quad \Phi(\Phi^*(\sigma)x) = \sigma\Phi(x),$$

for every $\sigma \in \text{Gal}(K)$ and for every $x \in F$ with $\Phi(x) \neq \infty$. The collection $\varphi^* = \{\Phi^* \mid \Phi \text{ prolongs } \varphi\}$ is a $\ker \alpha$ -inner-automorphism class.

When $E = K(\mathbf{T})$, $\mathbf{T} = (T_1, \dots, T_r)$, $r \geq 1$, and F is the splitting field of a polynomial $f(\mathbf{T}, X)$ that is separable in X we write $\mathcal{E}(f, K) = \mathcal{E}(F/E, K)$ and say that $\mathcal{E}(f, K)$ is the **associated embedding problem**. We emphasize that in this case $\text{Gal}(F/E) = \text{Gal}(f, K(\mathbf{T}))$ comes together with a natural permutation representation of degree $\deg_X f$.

Remark 2.1. Let $\mathbf{a} \in K^r$ be such that $f(\mathbf{a}, X)$ is separable and of the same degree as the X -degree of $f(\mathbf{T}, X)$. Then extend $\mathbf{T} \mapsto \mathbf{a}$ to a K -place of $K(\mathbf{T})$ with residue field K and let Φ be an L -place of F prolonging φ . Then $\Phi(x) \neq \infty$, for every root $x \in F$ of $f(\mathbf{T}, X)$. By (1) the action of $\text{Gal}(K)$ on the roots of $f(\mathbf{a}, X)$ coincides with the action of $\Phi^*(\text{Gal}(K))$ on the roots of $f(\mathbf{T}, X)$.

¹all homomorphism are assumed to be continuous

2.2. Double embedding problems. Let M/K be a field extension. A finite double embedding problem consists of a commutative diagram

$$(2) \quad \begin{array}{ccccc} & & \text{Gal}(M) & & \\ & \eta \swarrow & \downarrow r & \searrow \mu & \\ & & \text{Gal}(K) & & \\ & \theta \swarrow & \downarrow \nu & \searrow i & \\ B & \xrightarrow{j} & H & \xrightarrow{\beta} & G & \xleftarrow{i} & A \\ & \searrow \alpha & & & & & \end{array}$$

where G, H, A, B are finite groups, $B \leq H$, $A \leq G$, i, j are the inclusion maps, r is the restriction map, and α, μ, β, ν are surjective. Therefore a finite double embedding problem consists of two compatible finite embedding problem: (ν, β) for K and (μ, α) for M . In short we denote the double embedding problem by $((\mu, \alpha), (\nu, \beta))$.

A solution is a pair (η, θ) consisting of a weak solution η of (μ, α) and a weak solution θ of (ν, β) that commute (2). We note that $\eta = \theta r$, and that $(\theta r, \theta)$ is a solution if and only if $\theta(r(\text{Gal}(M))) \leq B$.

A finite double embedding problem is called rational if (ν, β) is rational. In that case, $H = \text{Gal}(F/K(\mathbf{T}))$ for some Galois extension $F/K(\mathbf{T})$, $G = \text{Gal}(L/K)$, where $L = F \cap K_s$, and α, ν are the restriction maps.

Then $A = \text{Gal}(L/L \cap M) \cong \text{Gal}(N/M)$, where $N = LM$, and B is a subgroup of $\beta^{-1}(A) = \text{Gal}(FN/M(\mathbf{T}))$. So $B \cong \text{Gal}(FN/E)$, for some $M(\mathbf{T}) \subseteq E \subseteq FN$. Under this identifications, α becomes the restriction map. Note that since α is surjective, $E \cap M_s = M$, and thus E is regular over M . So (μ, α) is a geometric embedding problem.

A geometric solution of a rational double embedding problem consists of a pair (Ψ^*, Φ^*) , where Ψ is an N -place of FN unramified over $M(\mathbf{T})$ such that the residue field of $K(\mathbf{T})$ is K and $\Phi = \Psi|_F$. In particular, Φ^* is a geometric solution of (ν, α) .

We note that if $f(\mathbf{T}, X) \in K[\mathbf{T}, X]$ is a separable polynomial, then $\mathcal{E}(f, M/K) = (\mathcal{E}(f, M), \mathcal{E}(f, K))$ is a finite rational double embedding problem for M/K .

2.3. The lifting property. We formulate the lifting property of PAC extensions [3, Proposition 4.6].

Proposition 2.2. *Let M/K be a PAC extension, let*

$$(\mathcal{E}_M, \mathcal{E}_K) = ((\mu: \text{Gal}(M) \rightarrow A, \alpha: B \rightarrow A), (\nu: \text{Gal}(K) \rightarrow G, \beta: H \rightarrow G))$$

be a rational finite double embedding problem for M/K and let η be a weak solution of \mathcal{E}_M . Then there exists a geometric solution (Ψ^, Φ^*) of $(\mathcal{E}_M, \mathcal{E}_K)$ such that $\Psi^* = \theta$.*

Moreover, if $H = \text{Gal}(F/K(\mathbf{T}))$, $\mathbf{T} = (T_1, \dots, T_r)$, and if $q(\mathbf{T}) \in K[\mathbf{T}]$ is nonzero, then we can choose Ψ so that $\mathbf{a} = \Psi(\mathbf{T}) \in K^r$, and $q(\mathbf{a}) \neq 0$.

3. PROOF OF THEOREM 1.2

Let K be a field, $\mathbf{T} = (T_1, \dots, T_r)$, $f_1(\mathbf{T}, X), \dots, f_s(\mathbf{T}, X) \in K[\mathbf{T}, X]$ distinct irreducible polynomials that are separable in X , $f = f_1 \cdots f_s$, and for each i let x_i be a root of $f_i(\mathbf{T}, X)$ in a fixed algebraic closure of $K(\mathbf{T})$. Let F be the splitting field of $f(\mathbf{T}, X)$ over $K(\mathbf{T})$, then $\hat{F} = FM$ is the splitting field of $f(\mathbf{T}, X)$ over $M(\mathbf{T})$. Let $L = F \cap K_s$ and $N = LM = FM \cap K_s$. Then the

associated double embedding problem $\mathcal{E}(f, M/K) = (\mathcal{E}(f, M), \mathcal{E}(f, K))$ is

$$\begin{array}{ccccc}
 & & \text{Gal}(M) & & \\
 & & \downarrow \varphi & \searrow \mu & \\
 & & \text{Gal}(K) & & \\
 & & \downarrow \nu & & \\
 \text{Gal}(\hat{F}/M(\mathbf{T})) & \xrightarrow{j} & \text{Gal}(F/K(\mathbf{T})) & \xrightarrow{\beta} & \text{Gal}(L/K) \xleftarrow{i} \text{Gal}(N/M). \\
 & \searrow \alpha & & &
 \end{array}$$

Here all maps are restriction maps. Note that $\ker(\alpha) \cong \ker(\beta) \cong \text{Gal}(FK_s/K_s(\mathbf{T}))$.

Let $\eta: \text{Gal}(M) \rightarrow \text{Gal}(\hat{F}/M(\mathbf{T}))$ be a weak solution of $\mathcal{E}(f, M)$. Let $H_0 = \eta(\text{Gal}(M))$ be the image of η . By the lifting property we have a Zariski dense set of $\mathbf{a} \in K^r$ and a geometric solution (Ψ^*, Φ^*) of $\mathcal{E}(f, M/K)$ such that $\Phi(\mathbf{T}) = \Psi(\mathbf{T}) = \mathbf{a}$ and $\Psi^* = \eta$. Let $H_1 = \theta(\text{Gal}(K))$; then $H_0 \leq H_1 \leq H := \text{Gal}(F/K(\mathbf{T}))$. Without loss of generality we can assume that $f(\mathbf{a}, X)$ is separable and of the same degree as $\deg_X f(\mathbf{T}, X)$, and hence the same holds true for all f_i .

Now all $f_i(\mathbf{a}, X)$ are irreducible if and only if $\text{Gal}(K)$ acts transitively on the set of roots of $f_i(\mathbf{a}, X)$ for all i . By Remark 2.1 the action of $\text{Gal}(K)$ on the roots of $f(\mathbf{a}, X)$ coincides with the action of H_1 on the roots of $f(\mathbf{T}, X)$. So it suffices to prove that H_1 acts transitively on the set of roots of $f_i(\mathbf{T}, X)$ which is Hx_i , for every i .

Let $\ker \alpha \leq C \leq \text{Gal}(f(\mathbf{T}, X), M(\mathbf{T}))$ and assume $(H_0 \cap C)x_i = Cx_i$ for every $i = 1, \dots, s$. Let $hx_i \in Hx_i$. Since $\beta(H_1) = \nu(\text{Gal}(K)) = \text{Gal}(L/K)$, we have $h_1 \in H_1$ such that $h_1^{-1}h \in \ker \beta = \ker \alpha \leq C$. So there exists $c \in H_0 \cap C$ such that $h_1^{-1}hx_i = cx_i$, hence $hx_i = (h_1c)x_i$. This finishes the proof since $h_1c \in H_1(H_0 \cap C) \leq H_1$. \square

4. APPLICATIONS

4.1. Proof of Theorem 1.6. Let K be a field of characteristic $p \geq 0$, let $f_1(T, X), \dots, f_s(T, X) \in K[T, X]$ be irreducible polynomials. Assume that the Zariski closure $C_i \subseteq \mathbb{P}^2$ of the affine curve $\{f_i = 0\} \subseteq \mathbb{A}^2$ is smooth for every $i = 1, \dots, s$ and that $p \nmid d_i(d_i - 1)$, where d_i is the total degree of f_i . Assume there exists a PAC extension M/K having a separable extension of degree d_i , for every $i = 1, \dots, s$. We have to show that there exist infinitely many $(a, b) \in K^2$ such that all $f_i(T, aT + b)$ are irreducible in $K[T]$.

In [6, Section 3] an open subset U of \mathbb{P}^2 is constructed such that for every $M \in U$ the compositum $\varphi_i: C_i \rightarrow \mathbb{P}^1$ of the inclusion map $C_i \rightarrow \mathbb{P}^2 \setminus \{M\}$ and of the projection from M map $\mathbb{P}^2 \setminus \{M\} \rightarrow \mathbb{P}^1$ is a degree d_i map having the following property. If $F_i/K(X)$ is the Galois closure of the function field extension corresponding to φ_i , then $\text{Gal}(F_iK_s/K_s(X)) \cong S_{d_i}$. Moreover, if $F = F_1 \cdots F_s$, then $\text{Gal}(FK_s/K_s(X)) \cong \prod_{i=1}^s S_{d_i}$. (Note that we switched the roles of X, T here, in order to be consistent with the notation of [6].)

Choosing affine coordinates, we get that there exist nonzero $a_1, a_2, a_3, a_4, a_5 \in K$ such that $F_i/K(X)$ is the splitting field of the polynomial $\tilde{f}_i(T, X) = f_i(T, \frac{a_1T + a_2X + a_3}{a_4X + a_5})$, for every $i = 1, \dots, s$. Let $f(T, X) = \prod_{i=1}^s \tilde{f}_i$, then $\text{Gal}(f, K(X)) \cong \text{Gal}(f, M(X)) \cong \text{Gal}(f, K_s(X)) \cong \prod_{i=1}^s S_{d_i}$, where the i th coordinate permutes the roots of \tilde{f}_i , for every i . Therefore

$$\mathcal{E}(f, M) = \left(\nu: \text{Gal}(M) \rightarrow \prod_{i=1}^s S_{d_i}, \alpha: \prod_{i=1}^s S_{d_i} \rightarrow 1 \right).$$

Let M_i/M be a separable extension of degree d_i , for every $i = 1, \dots, s$. Then $\text{Gal}(M)$ acts transitively on $\text{Hom}_M(M_i, M_s)$, which is a set of cardinality d_i . So it induces a homomorphism $\eta: \text{Gal}(M) \rightarrow \text{Gal}(f(T, X), M(X)) \cong \prod_{i=1}^s S_{d_i}$ that acts transitively on the roots of $\tilde{f}_i(T, X)$, for all i . Then the assumptions of Theorem 1.2 are satisfied (see also Remark 2.1). We thus get infinitely many specializations $X \mapsto b_0 \in K$ such that $\tilde{f}_i(T, b_0) = f_i(T, aT + b)$ is irreducible, for every i , where $a = \frac{a_1}{a_4b_0 + a_5}$ and $b = \frac{a_2b_0 + a_3}{a_4b_0 + a_5}$. \square

4.2. Theorem 1.6 for large finite fields. We show how Theorem 1.6 implies the following theorem of Bender-Wittenberg.

Theorem 4.1 (Bender-Wittenberg). *Let A, B be positive integers, p a prime, q a power of p , and let $f_1(T, X), \dots, f_s(T, X) \in \mathbb{F}_q[T, X]$ be irreducible polynomials of respective total degrees d_1, \dots, d_s such that $\sum d_i \leq B$. Assume*

- (a) $p \nmid d_i(d_i - 1)$, for all i ,
- (b) the Zariski closure C_i of the affine curve $\{f_i = 0\}$ in \mathbb{P}^2 is smooth, and
- (c) $q \gg A, B$.

Then there exist at least A pairs $(a, b) \in \mathbb{F}_q^2$ for which all $f_i(T, aT + b)$ are irreducible.

Proof. We fix A, B . Then the following statement is elementary in the language of rings.

Σ : Every family of irreducible polynomials $f_1(T, X), \dots, f_s(T, X) \in K[T, X]$ of respective total degrees d_1, \dots, d_s such that $d_i(d_i - 1) \neq 0$ in K , and the Zariski closure C_i of the affine curve $\{f_i = 0\}$ in \mathbb{P}^2 is smooth admits at least A pairs $(a, b) \in K^2$ such that all $f_i(T, X)$ are irreducible.

Let K a pseudo finite field. In terms of PAC extensions this means that K/K is a PAC extension, K perfect, and $\text{Gal}(K) = \widehat{\mathbb{Z}}$. In particular, K has a separable extension of degree n , for every $n \geq 1$. So, by Theorem 1.6, K satisfies Σ . By Ax' theorem on the elementary theory of finite fields [8, Proposition 20.10.4] we get that all but finitely many finite fields satisfies Σ , as needed. \square

4.3. Proof of Theorem 1.7. Let K be a field of characteristic $p \geq 0$, let $n \geq 1$ be an integer such that n is odd if $p = 2$, and let $f_1(X), \dots, f_s(X) \in K[X]$ be non-associate irreducible separable polynomials with respective roots $\omega_1, \dots, \omega_s$. Assume there exists a PAC extension M/K such that $M(\omega_i)$ has a degree n separable extension, for every $i = 1, \dots, s$. We need to prove that there exists a Zariski dense set of $(a_1, \dots, a_n) \in K^n$ such that for $g(T) = T^n + a_1T^{n-1} + \dots + a_n$ all $f_i(g(T))$ are irreducible.

Let $f = f_1 \cdots f_s$, let $\mathbf{A} = (A_1, \dots, A_n)$ be an n -tuple of algebraically independent variables and let

$$\mathcal{G}(\mathbf{A}, T) = T^n + A_1T^{n-1} + \dots + A_n.$$

Let F be the splitting field of $f \circ \mathcal{G}(\mathbf{A}, T)$ over $K(\mathbf{A})$ and L be the splitting field of f over K . Then since n is odd if $p = 2$, [4, Proposition 3.6] gives that F is regular over L and

$$\text{Gal}(F/K(\mathbf{A})) \cong S_n \wr_{\Omega} \text{Gal}(L/K),$$

as permutation groups. Here the LHS acts on the set Φ of roots of $f \circ \mathcal{G}(\mathbf{A}, T)$ in some algebraic closure of $K(\mathbf{A})$, $S_n \wr_{\Omega} \text{Gal}(L/K) \cong S_n^{\Omega} \rtimes \text{Gal}(L/K)$ is the permutational wreath product that acts on the set $\{1, \dots, n\} \times \Omega$, where Ω is the set of roots of f .

Similarly $\text{Gal}(f \circ \mathcal{G}(\mathbf{A}, T), M(\mathbf{A})) = \text{Gal}(FM/M(\mathbf{A})) = S_n \wr_{\Omega} \text{Gal}(N/M)$, where $N = LM$ is the splitting field of f over M . So

$$\mathcal{E}(f \circ \mathcal{G}, M) = (\nu: \text{Gal}(M) \rightarrow \text{Gal}(N/M), \alpha: S_n \wr_{\Omega} \text{Gal}(N/M) \rightarrow \text{Gal}(N/M)),$$

where α is the quotient map. Note that $\ker \alpha = S_n^{\Omega}$.

Let $\Omega_1, \dots, \Omega_s$ be the $\text{Gal}(N/M)$ -orbits of Ω , so $S \geq s$. Assume that $\omega_i \in \Omega_i$, for $i = 1, \dots, s$. By assumption, for each $i = 1, \dots, s$, we have a tower of separable extensions $M \subseteq M(\omega_i) \subseteq M_i$ and $[M_i : M(\omega_i)] = n$. For $i = s+1, \dots, S$, let $M_i = M(\omega_i)$, for some $\omega_i \in \Omega_i$.

Let R be the minimal Galois extension of M that contains all M_i . Then by [4, Lemma 3.7] we have a homomorphism $\rho: \text{Gal}(R/M) \rightarrow S_n \wr_{\Omega} \text{Gal}(N/M)$ such that $\alpha(\rho(\sigma)) = \sigma|_N$ and if we denote by H_0 the image of ρ , then H_0 acts transitively on $\{1, \dots, n\} \times \Omega_i$, for $i = 1, \dots, s$.

Let C be the stabilizer of $\{1, \dots, n\} \times \Omega_i$ in $S_n \wr_{\Omega} \text{Gal}(N/M)$. Then $\ker \alpha = S_n^{\Omega} \leq C$ and $H_0 \leq C$. We have

$$(H_0 \cap C)(1, \omega_i) = H_0(1, \omega_i) = \{1, \dots, n\} \times \Omega_i = C(1, \omega_i).$$

By Theorem 1.2, there exists a Zariski dense set of $\mathbf{a} \in K^n$ such that all $f_i(g(T))$ are irreducible, where $g(T) = \mathcal{G}(\mathbf{a}, T) = T^n + a_1T^{n-1} + \dots + a_n$. \square

4.4. Theorem 1.7 for large finite fields. An argument similar to that used in Section 4.2 can be applied to deduce a result for large finite fields out of Theorem 1.7. In [4] a more precise statement was proved for pseudo finite fields, that gives the stronger result over finite fields that was stated in Remark 1.8.

4.5. Proof of Theorem 1.9. Let K be a field. Assume that for infinitely many $n \geq 1$ there exists a PAC extension M/K with $\text{Gal}(M)$ free of rank $\geq n$. We have to show that K is Hilbertian.

Let $f(T, X) \in K[T, X]$ be an irreducible polynomial. Let $G = \text{Gal}(f(T, X), K(T))$. By assumption, there exists a PAC extension M/K such that $\text{Gal}(M)$ is a free profinite group of rank $r \geq |G|$. In particular $r \geq \text{rank}(\text{Gal}(f(T, X), M(T)))$, so the associated embedding problem

$$\mathcal{E}(f, M) = (\nu: \text{Gal}(M) \rightarrow \text{Gal}(N/M), \alpha: \text{Gal}(f(T, X), M(T)) \rightarrow \text{Gal}(N/M))$$

is properly solvable [8, Proposition 17.7.3 and Theorem 24.8.1], so by Theorem 1.2 (see Remark 1.8) there exists an element $a \in K$ for which $f(a, X)$ is irreducible. Thus K is Hilbertian. \square

REFERENCES

1. James Ax, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271. MR MR0229613 (37 #5187)
2. Lior Bary-Soroker, *Dirichlet’s theorem for polynomial rings*, Proc. Amer. Math. Soc. **137** (2009), no. 1, 73–83,
3. Lior Bary-Soroker, *On pseudo algebraically closed extensions of fields*, Journal of Algebra **322** (2009), no. 6, 2082–2105.
4. ———, *Irreducible values of polynomials*, 2010, arXiv:1005.4528
5. Lior Bary-Soroker and Dubi Kelmer, *On PAC extensions and scaled trace forms*, Israel Journal of Mathematics, **175** (2010) no. 1, 113–124.
6. Andreas O. Bender and Olivier Wittenberg, *A potential analogue of Schinzel’s hypothesis for polynomials with coefficients in $\mathbb{F}_q[t]$* , Int. Math. Res. Not. (2005), no. 36, 2237–2248. MR MR2181456 (2006g:11230)
7. Brian Conrad, Keith Conrad, and Robert Gross, *Prime specialization in genus 0*, Trans. Amer. Math. Soc. **360** (2008), no. 6, 2867–2908. MR MR2379779 (2009b:11166)
8. Michael D. Fried and Moshe Jarden, *Field arithmetic*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008, Revised by Jarden. MR MR2445111
9. Dan Haran, *Hilbertian fields under separable algebraic extensions*, Invent. Math. **137** (1999), no. 1, 113–126. MR MR1702139 (2001a:12006)
10. Moshe Jarden and Aharon Razon, *Pseudo algebraically closed fields over rings*, Israel J. Math. **86** (1994), no. 1-3, 25–59. MR MR1276130 (95c:12006)
11. Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999. MR MR1711577 (2000k:12004)
12. Paul Pollack, *Simultaneous prime specializations of polynomials over finite fields*, Proc. Lond. Math. Soc. (3) **97** (2008), no. 3, 545–567. MR MR2448239 (2009f:11155)
13. Aharon Razon, *Abundance of Hilbertian domains*, Manuscripta Math. **94** (1997), no. 4, 531–542. MR MR1484642 (98h:12002)
14. Winfried Scharlau, *On trace forms of algebraic number fields*, Math. Z. **196** (1987), no. 1, 125–127. MR MR907414 (88h:11024)
15. Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992, Lecture notes prepared by Henri Damon [Henri Darmon], With a foreword by Darmon and the author. MR MR1162313 (94d:12006)
16. Helmut Völklein, *Groups as Galois groups*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996, An introduction. MR MR1405612 (98b:12003)
17. William C. Waterhouse, *Discriminants of étale algebras and related structures*, J. Reine Angew. Math. **379** (1987), 209–220. MR MR903641 (89a:11046)

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK, UNIVERSITÄT DUISBURG-ESSEN, ELLERNSTRASSE 29, D-45326 ESSEN, GERMANY

E-mail address: lior.bary-soroker@uni-due.de